CHAPTER 1

# Overview

This chapter provides an overview of the Cisco Connected Grid10-Port Ethernet Switch Module Interface Card (also known as a switch module or the CGR 2010 ESM). This chapter contains the following topics:

**Note** In this document, *IP* refers to IP Version 4 (IPv4) unless otherwise specified as IPv6.

## Introduction

The CGR 2010 ESM is designed for internetworking in the energy industry, typically in power substations for substation automation and integration, as well as harsh environments such as electric substation environments, intelligent transportation trackside substations, downstream oil and gas, and other Connected Energy applications.

The CGR 2010 ESM is a double-wide switch module that is installed into the Cisco CGR 2010 router chassis. There are two models for this switch module:

***Table 1-1 CGR 2010 ESM Copper Model***

| Model | Description |
|---|---|
| GRWIC-D-ES-2S-8PC (Copper model) | 8x 10/100 Fast Ethernet ports, 1x dual-purpose port (10/100/1000 Base-T copper RJ-45 and 100/1000 SFP fiber), 1x 100/1000 SFP fiber-only port |

*Figure 1-1 GRWIC-D-ES-2S-8PC (Copper Model)*

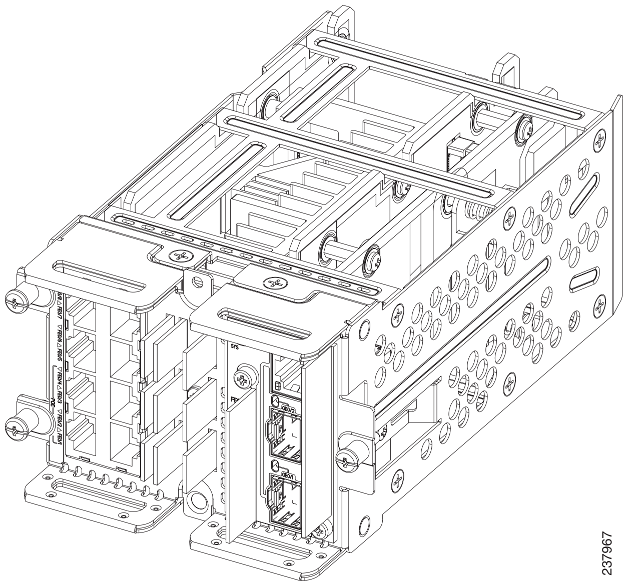
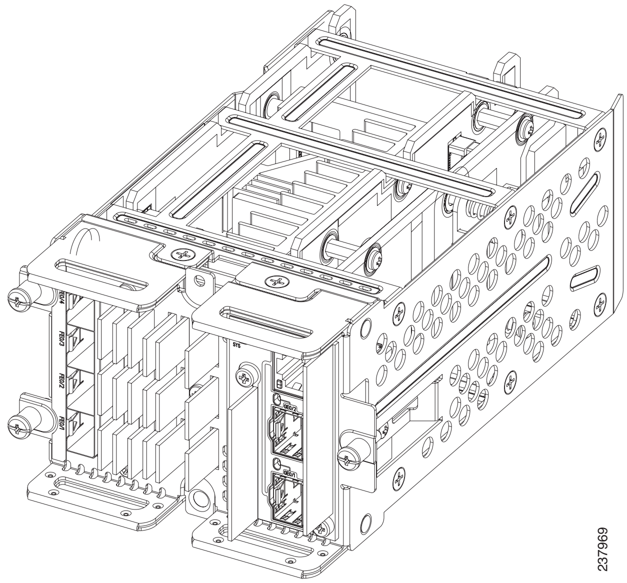


*Table 1-2 CGR 2010 ESM SFP Fiber Model*

| Model | Description |
|---|---|
| GRWIC-D-ES-6S (SFP Fiber model) | 4x 100BASE-FX SFP-module ports, 1x dual-purpose port (1x 10/100/1000Base-T copper RJ-45 port and 1x 100/1000 SFP fiber module port), 1x 100/1000 SFP fiber module port |

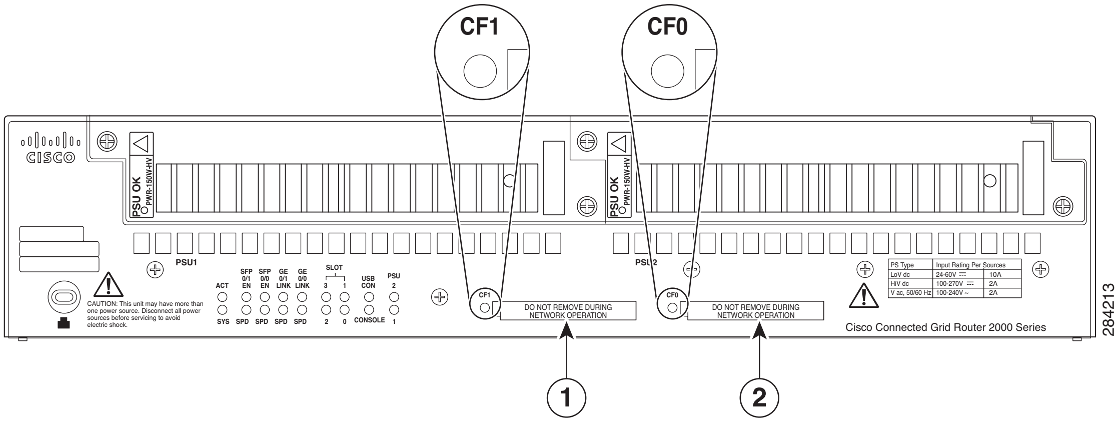
*Figure 1-2 GRWIC-D-ES-6S (SFP Fiber Model)*



# Router Compact Flash Memory Cards

The router supports a maximum of two compact flash memory cards. The router ships with one compact flash card installed and supports a second, optional flash card that you can order with the router or supply separately. Figure 1-3 illustrates the location of the compact flash card slots on the router.

*Figure 1-3 Cisco Connected Grid 2010 Router—Compact Flash Memory Card Slot Locations*



| Item | Label on Router | Description | Cisco IOS Interface Name |
|---|---|---|---|
| 1 | CF1 | This slot supports an optional compact flash card that you can order with the router or supply separately. The Connected Grid Swap Drive feature is not supported on this slot. | **flash1:** |
| 2 | CF0 | This is the required slot for use with the Connected Grid Swap Drive feature. The router comes with a compact flash card already installed in this slot.<br>The Connected Grid Swap Drive feature is supported on this CF slot only. | **flash** or **flash0**: |

For additional information about the router compact flash memory support, refer to the router hardware installation guide at:

http://www.cisco.com/en/US/products/ps10977/prod_installation_guides_list.html

# Detecting and Validating the Switch Module

When you install the CGR 2010 ESM into the double-wide slot on the Cisco CGR 2010 router, the router identifies and validates the switch module.

## Communication Between the Host Router and the Switch Module

The backplane interface on the CGR 2010 ESM is called *PortChannel48*. The backplane interface on the host router side is called **GigabitEthernet0/x/0** (interface **GigabitEthernet0/0/0** and/or interface **GigabitEthernet0/2/0**). The backplane interface provides communication between the host router and the switch module.

If the switch module is installed in slot0 of the CGR 2010 router, the interface **GigabitEthernet0/0/0** is created automatically. GigabitEthernet0/0/0 is the backplane interface connected to the switch module in slot0. This interface supports creation of subinterfaces for inter-VLAN routing functionality.

The PortChannel48 interface consists of eight 10/100 FastEthernet physical links that are grouped together to create a FastEtherChannel. For details, see Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."

## Removing the Switch Module

Online Insertion and Removal (OIR) of the CGR 2010 ESM is not supported. For information on the correct procedure for removing the switch module from the router, see "Removing the Switch Module" in the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*.

**Caution** The Cisco CGR 2010 router does not support removing switch modules when the chassis is powered on. Removing the switch module when the router is running can result in undesirable behavior, such as resetting or damaging to the router.

### About Router Reset and the Switch Module

The CGR 2010 ESM is a GRWIC (Grid Router WAN Interface Card) inserted into the Cisco CGR 2010 router. When the router crashes or the router is reloaded gracefully, the switch module remains up and running. In this state, the backplane interface is down, but the switch module can still occur between the front panel ports.

When the router starts to load the image (either through the manual or autoboot process), the router resets the switch module.

**Caution** Any unsaved configurations on the switch module will be lost if the CGR 2010 router is reloaded. Make sure you write the configurations to NVRAM on the switch module using the **write memory** command.

## Switch Module Software Images and Interface Types

The CGR 2010 ESM ships with one of these software images installed:

- **CGR 2010 LAN base image:** This image includes advanced Quality of Service (QoS), flexible VLAN handling, Supervisory Control and Data Acquisition (SCADA) protocol classification support, Resilient Ethernet Protocol (REP) for improved convergence time in ring topologies, Flexlink for fast failover in hub-and-spoke topologies, and comprehensive security features.

- **CGR 2010 IP services image:** In addition to features supported in the LAN based image, this adds advanced Layer 3 features, such as support for advanced IP routing protocols, Multi-VPN Routing and Forwarding Customer Edge (Multi-VRF CE/VRF-Lite), and Policy Based Routing (PBR).

The swtich has three different types of interfaces:

- Network Node Interfaces (NNIs)—connects to the service provider network
- User Network Interfaces (UNIs)—connects to customer networks
- Enhanced Network Interfaces (ENIs)—an ENI is typically a user-network facing interface and has the same default configuration and functionality as UNIs, but can be configured to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP).

**Note** By default, on startup, all ports on the switch module are enabled as NNIs. The default status for an NNI is administratively up to allow a service provider remote access to the switch module during initial configuration.

# Switch Module Features

This section describes the following features:

- Performance Features, page 1-5
- Management Options, page 1-6
- Manageability Features, page 1-7

## Performance Features

The CGR 2010 ESM provides the following performance features:

- Autosensing of port speed and auto negotiation of duplex mode on all switch module ports for optimizing bandwidth
- Automatic-medium dependent interface crossover (auto-MDIX) capability on 10/100 and 10/100/1000 Mbps interfaces that enable the interface to automatically detect the required cable connection type (straight-through or crossover), and to configure the connection appropriately.
- Support for routed frames up to 1998 bytes, for frames up to 9000 bytes that are bridged in hardware, and for frames up to 2000 bytes that are bridged by software
- IEEE 802.3x flow control on all ports (the switch module does not send pause frames)
- EtherChannel for enhanced fault tolerance and for providing up to 800 Mbps (Fast EtherChannel) full duplex of bandwidth between the switch modules, routers, and servers
- Forwarding of Layer 2 and Layer 3 packets at Gigabit line rate
- Per-port storm control for preventing broadcast, multicast, and unicast storms
- Port blocking on forwarding unknown Layer 2 unknown unicast, multicast, and bridged broadcast traffic
- Internet Group Management Protocol (IGMP) snooping for IGMP versions 1, 2, and 3 for efficiently forwarding multimedia and multicast traffic

- IGMP report suppression for sending only one IGMP report per multicast router query to the multicast devices (supported only for IGMPv1 or IGMPv2 queries)
- IGMP snooping querier support to configure the switch module to generate periodic IGMP General Query messages
- IGMP Helper to allow the switch module to forward a host request to join a multicast stream to a specific IP destination address (requires the IP services image)
- IGMP filtering for controlling the set of multicast groups to which hosts on a switch module port can belong
- IGMP throttling for configuring the action when the maximum number of entries is in the IGMP forwarding table
- IGMP configurable leave timer to configure the network's leave latency
- Multicast VLAN registration (MVR) to continuously send multicast streams in a multicast VLAN while isolating the streams from subscriber VLANs for bandwidth and security reasons with support for 512 multicast entries on a switch module
- MVR over trunk port (MVRoT) support to allow you to configure a trunk port as an MVR receiver port
- Multicast VLAN Registration (MVR) enhancements include the ability to configure 2000 MVR groups when the switch module is in dynamic MVR mode and a command (**mvr ringmode flood**) to ensure that forwarding in a ring topology is limited to member ports
- Switch Database Management (SDM) templates for allocating system resources to maximize support for user-selected features, including the dual-ipv4-and-ipv6 template for supporting IPv6 addresses
- RADIUS server load balancing to allow access and authentication requests to be distributed evenly across a server group

# Management Options

The CGR 2010 ESM provides the following management features:

- **Command Line Interface** (CLI)—Cisco IOS software supports desktop-switching and multilayer-switching features

  Before you can access the switch module CLI, you must connect to the Cisco CGR 2010 router through the router console or through Telnet. Once you are connected to the Cisco CGR 2010 router, you must configure an IP address on the backplane Gigabit Ethernet interface connected to the switch module.

  To connect to the router, open a session to the switch module using the **service-module gigabitethernet** *0/x/0* **session** command in privileged EXEC mode on the router.

  For detailed information about using this CLI, see Chapter 3, "Access the Switch Module from the Host Router."
- **Cisco Configuration Engine**—Network management device that works with embedded Cisco IOS CNS Agents in the switch module software. You can automate initial configurations and configuration updates by generating switch module-specific configuration changes, sending them to the switch module, executing the configuration change, and logging the results. For more information about using Cisco IOS agents, see Chapter 5, "Cisco IOS Configuration Engine."

- **Cisco Configuration Professional**—GUI-based device management tool for Cisco access routers. It simplifies router, firewall, IPS, VPN, unified communications, WAN, and basic LAN configuration through easy-to-use wizards.
- **SNMP**—Includes SNMP management applications such as CiscoWorks2000 LAN Management Suite (LMS) and HP OpenView. You can manage from an SNMP-compatible management station that is running platforms such as HP OpenView or SunNet Manager. The switch module supports a comprehensive set of MIB extensions, and four remote monitoring (RMON) groups. For more information about using SNMP, see Chapter 14, "Quality of Service Configuration."

## Manageability Features

The CGR 2010 ESM provides the following manageability features:

**Note** The encrypted Secure Shell (SSH) feature listed in this section is available only on the cryptographic versions of the switch module software image.

- MODBUS TCP support to connect to devices such as Intelligent Electronic Devices (IEDs), distributed controllers, substation routers, Cisco IP Phones, Cisco Wireless Access Points, and other network devices (such as redundant substation switches modules).
- Support for classification and prioritization of Generic Object-Oriented Substation Events (GOOSE) messages and SCADA messages, using QoS functionality
- Cisco-default Smart port macros for creating custom switch module configurations for simplified deployment across the network
- Express Setup for quickly configuring a switch module for the first time with basic IP information, contact information, switch module and Telnet passwords, and Simple Network Management Protocol (SNMP) information through a browser-based program. For more information about Express Setup, see "Running Express Setup" in the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*.
- Support for DHCP for configuration of switch module information (such as IP address, default gateway, hostname, and Domain Name System [DNS] and TFTP server names)
- DHCP relay for forwarding User Datagram Protocol (UDP) broadcasts, including IP address requests, from DHCP clients
- DHCP server for automatic assignment of IP addresses and other DHCP options to IP hosts
- DHCP-based auto-configuration and image update to download a specified configuration a new image to a large number of switch modules
- DHCP server port-based address allocation for the preassignment of an IP address to a switch module port
- Directed unicast requests to a DNS server for identifying a switch module through its IP address and its corresponding hostname, and to a TFTP server for administering software upgrades from a TFTP server
- Address Resolution Protocol (ARP) for identifying a switch module through its IP address and its corresponding MAC address
- Unicast MAC address filtering to drop packets with specific source or destination MAC addresses
- Configurable MAC address scaling that allows disabling MAC address learning on a VLAN to limit the size of the MAC address table

- Cisco Discovery Protocol (CDP) Versions 1 and 2 for network topology discovery and mapping between the switch module and other Cisco devices on the network (supported on NNIs by default, can be enabled on ENIs, but not supported on UNIs)
- Link Layer Discovery Protocol (LLDP) and LLDP Media Endpoint Discovery (LLDP-MED) for interoperability with third-party IP phones (supported only on NNIs or ENIs)
- Support for the LLDP-MED location TLV that provides location information from the switch module to the endpoint device
- Network Time Protocol (NTP) for providing a consistent timestamp to all switch modules from an external source
- Cisco IOS File System (IFS) for providing a single interface to all file systems that the switch module uses
- In-band management access for up to 16 simultaneous Telnet connections for multiple CLI-based sessions over the network
- In-band management access for up to five simultaneous, encrypted Secure Shell (SSH) connections for multiple CLI-based sessions over the network (requires the cryptographic versions of the switch module software)
- In-band management access through SNMP Versions 1, 2c, and 3 get and set requests
- Out-of-band management access through the Cisco CGR 2010 router console port to a directly attached terminal, or to a remote terminal through a serial connection or a modem
- Support for metro Ethernet operation, administration, and maintenance (OAM) IEEE 802.1ag Connectivity Fault Management (CFM), Ethernet Line Management Interface (E-LMI) on customer-edge and provider-edge switch modules, and 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback, and 802.3ah Ethernet OAM discovery, link monitoring, remote fault detection, and remote loopback
- Support for Ethernet loopback facility for testing connectivity to a remote device including VLAN loopback for non-disruptive loopback testing, and terminal loopback to test full-path QoS in both directions (requires the IP services image)
- Configuration replacement and rollback to replace the running configuration on a switch module with any saved Cisco IOS configuration file
- Source Specific Multicast (SSM) mapping for multicast applications to provide a mapping of source to allow IGMPv2 clients to utilize SSM, and allow listeners to connect to multicast sources dynamically and reduce dependencies on the application
- HTTP client can send requests to both IPv4 and IPv6 HTTP servers, and the HTTP server in Cisco IOS can service HTTP requests from both IPv4 and IPv6 HTTP clients (requires the IP services image)
- IPv6 supports stateless auto-configuration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses (requires the IP services image)
- IPv6 supports stateless auto-configuration to manage link, subnet, and site addressing changes, such as management of host and mobile IP addresses (requires the IP services image)
- CPU utilization threshold trap monitors CPU utilization
- Support for including a hostname in the option 12 field of DHCPDISCOVER packets, providing identical configuration files to be sent by using the DHCP protocol
- DHCP Snooping enhancement to support the selection of a fixed string-based format for the circuit-id sub-option of the Option 82 DHCP field

## Availability Features

The CGR 2010 ESM provides the following availability features:

- UniDirectional Link Detection (UDLD) and aggressive UDLD for detecting and disabling unidirectional links on fiber-optic interfaces caused by incorrect fiber-optic wiring or port faults
- 802.1D Spanning Tree Protocol (STP) for redundant backbone connections and loop-free networks (supported by default on NNIs, can be enabled on ENIs, not supported on UNIs). STP has these features:
  - Up to 128 supported spanning-tree instances
  - Per-VLAN spanning-tree plus (PVST+) for balancing load across VLANs
  - Rapid PVST+ for balancing load across VLANs and providing rapid convergence of spanning-tree instances
- 802.1s Multiple Spanning Tree Protocol (MSTP) on NNIs or ENIs for grouping VLANs into a spanning-tree instance, providing multiple forwarding paths for data traffic and load balancing, and providing rapid per-VLAN Spanning-Tree plus (rapid-PVST+) based on the IEEE 802.1w Rapid Spanning Tree Protocol (RSTP) for rapid convergence of the spanning tree (by immediately transitioning root and designated port NNIs or spanning-tree enabled ENIs to the forwarding state)
- Optional spanning-tree features available in PVST+, rapid-PVST+, and MSTP modes on NNIs and ENIs, where spanning tree has been enabled:
  - Port Fast for eliminating the forwarding delay by enabling a spanning-tree port to immediately transition from the blocking state to the forwarding state
  - Bridge protocol data unit (BPDU) guard for shutting down Port Fast-enabled ports that receive BPDUs
  - BPDU filtering for preventing a Port Fast-enabled ports from sending or receiving BPDUs
  - Root guard for preventing switch modules outside the network core from becoming the spanning-tree root
  - Loop guard for preventing alternate or root port NNIs or ENIs from becoming designated ports because of a failure that leads to a unidirectional link
- Flex Link Layer 2 interfaces to backup one another as an alternative to STP for basic link redundancy in a nonloop network with pre-emptive switchover and bidirectional fast convergence; also referred to as the MAC address-table move update feature
- Flex Link Multicast Fast Convergence to reduce the multicast traffic convergence time after a Flex Link failure
- Link-state tracking to mirror the state of the ports that carry upstream traffic from connected hosts and servers, and to allow the failover of the server traffic to an operational link on another CGR 2010 ESM
- Support for Resilient Ethernet Protocol (REP) for improved convergence times and network loop prevention without the use of spanning tree
- Counter and timer enhancements to REP support
- Support for REP edge ports when the neighbor port is not REP-capable
- HSRP for Layer 3 router redundancy (requires IP services image)
- Equal-cost routing for link-level and switch module-level redundancy (requires IP services image)
- Shorter Resilient Ethernet Protocol (REP) hello: Changes the range of the REP link status layer (LSL) age timer from 3000 to 10000 ms in 500-ms intervals to 120 to 10000 ms in 40-ms intervals

## VLAN Features

The CGR 2010 ESM provides the following VLAN features:

- Support for up to 1005 VLANs for assigning users to VLANs associated with appropriate network resources, traffic patterns, and bandwidth
- Support for VLAN IDs in the full 1 to 4094 range allowed by the 802.1Q standard
- VLAN Query Protocol (VQP) for dynamic VLAN membership
- 802.1Q trunking encapsulation on all ports for network moves, adds, and changes; management and control of broadcast and multicast traffic; and network security by establishing VLAN groups for high-security users and network resources
- VLAN 1 minimization for reducing the risk of spanning-tree loops or storms by allowing VLAN 1 to be disabled on any individual VLAN trunk link. With this feature enabled, no user traffic is sent or received on the trunk. The switch module CPU continues to send and receive control protocol frames.
- UNI-ENI isolated VLANs to isolate customer VLANs from VLANs of other customers on the same switch. Local switching does not occur among UNIs or ENIs on the switch module that belongs to the same UNI-ENI isolated VLAN.
- Private VLANs to address VLAN scalability problems, to provide a more controlled IP address allocation, and to allow Layer 2 ports to be isolated from ports on other switch modules
- Port security on a PVLAN host to limit the number of MAC addresses learned on a port, or define which MAC addresses may be learned on a port
- VLAN Flex Link Load Balancing to provide Layer 2 redundancy without requiring Spanning Tree Protocol (STP). A pair of interfaces configured as primary and backup links can load balance traffic based on VLAN.

## Security Features

**Note** The CGR 2010 ESM provides security for the subscriber, the switch module, and the network.

The CGR 2010 ESM provides the security features, as described below.

### Subscriber Security

- By default, local the switch module is disabled among subscriber ports to ensure that subscribers are isolated
- DHCP snooping to filter untrusted DHCP messages between untrusted hosts and DHCP servers
- DHCP Snooping Statistics **show** and **clear** commands to display and remove DHCP snooping statistics in summary or detail form
- IP source guard to restrict traffic on nonrouted interfaces by filtering traffic based on the DHCP snooping database and IP source bindings
- Dynamic ARP inspection to prevent malicious attacks on the switch module by not relaying invalid ARP requests and responses to other ports in the same VLAN

## Switch Module Security

**Note** The Kerberos feature listed in this section is only available on the cryptographic version of the switch module software.

- Password-protected access (read-only and read-write access) to management interfaces for protection against unauthorized configuration changes
- Configuration file security so that only authenticated and authorized users have access to the configuration file, preventing users from accessing the configuration file by using the password recovery process
- Multi-level security for a choice of security level, notification, and resulting actions
- Port security option for limiting and identifying MAC addresses of the stations allowed to access the port
- Port security aging to set the aging time for secure addresses on a port
- LLDP (Link Layer Discovery Protocol) and LLLDP-MED (Media Extensions)—Adds support for 802.1AB link layer discovery protocol for interoperability in multi-vendor networks. Switches exchange speed, duplex, and power settings with end devices such as IP phones.
- UNI and ENI default port state is disabled
- Automatic control-plane protection to protect the CPU from accidental or malicious overload due to Layer 2 control traffic on UNIs or ENIs
- Configurable control plane security that provides service providers with the flexibility to drop customers control-plane traffic on a per-port, per-protocol basis. Allows configuring of ENI protocol control packets for CDP, STP, LLDP, and LACP.
- TACACS+, a proprietary feature for managing network security through a TACACS server
- RADIUS for verifying the identity of, granting access to, and tracking the actions of remote users through Authentication, Authorization and Accounting (AAA) services
- Kerberos security system to authenticate requests for network resources by using a trusted third-party (requires the cryptographic version of the switch module software)

## Network Security

- Static MAC addressing for ensuring security
- Standard and extended IP Access Control Lists (ACLs) for defining security policies in both directions on routed interfaces (router ACLs) and VLANs and inbound on Layer 2 interfaces (port ACLs)
- IPv6 ACLs to be applied to interfaces to filter IPv6 traffic
- Extended MAC access control lists for defining security policies in the inbound direction on Layer 2 interfaces
- VLAN ACLs (VLAN maps) for providing intra-VLAN security by filtering traffic based on information in the MAC, IP, and TCP/UDP headers
- Source and destination MAC-based ACLs for filtering non-IP traffic
- 802.1x port-based authentication to prevent unauthorized devices (clients) from gaining access to the network, including the following features:

  - VLAN assignment for restricting 802.1x-authenticated users to a specified VLAN
  - Port security for controlling access to 802.1x ports
  - 802.1x accounting to track network usage
  - 802.1x readiness check to determine the readiness of connected end hosts before configuring 802.1x on the switch module
  - Network Edge Access Topology (NEAT) with 802.1x switch module supplicant, host authorization with Client Information Signalling Protocol (CISP), and auto-enablement to authenticate a switch module outside a wiring closet as a supplicant to another switch module
- Support for IP source guard on static hosts
- 802.1x User Distribution to allow deployments with multiple VLANs (for a group of users) to improve scalability of the network by load balancing users across different VLANs. Authorized users are assigned to the least populated VLAN in the group, assigned by RADIUS server.
- Support for 3DES and AES with version 3 of the Simple Network Management Protocol (SNMPv3). This release adds support for the 168-bit Triple Data Encryption Standard (3DES) and the 128-bit, 192-bit, and 256-bit Advanced Encryption Standard (AES) encryption algorithms to SNMPv3.
- Additional IPv6 support to include IPv6 eBGP, IPv6 SNMP, Syslog, and HTTP as well as IPv6 MLD snooping

## QoS and CoS Features

The CGR 2010 ESM provides the following Quality of Service (QoS) and Class of Service (CoS) features:

- QoS features for implementing high-priority (low-latency) traffic via backplane between the switch module and the host CGR 2010 router. S*ee "Implementing High-Priority Traffic to the Host Router" section on page 14-95*. For more information, see also Chapter 9, "EtherChannel Configuration Between the Switch Module and the Host Router."
- Configurable control-plane queue assignment to assign control plane traffic for CPU-generated traffic to a specific egress queue
- Cisco Modular QoS Command-line (MQC) implementation
- Classification based on IP precedence, Differentiated Services Code Point (DSCP), and 802.1p CoS packet fields, ACL lookup, or assigning a QoS label for output classification
- Policing:
  - One-rate policing based on average rate and burst rate for a policer
  - Two-color policing that allows different actions for packets that conform to or exceed the rate
  - Aggregate policing for policers shared by multiple traffic classes
- Weighted Tail Drop (WTD) as the congestion-avoidance mechanism for managing the queue lengths and providing drop precedences for different traffic classifications
- Table maps for mapping DSCP, CoS, and IP precedence values
- Queuing and scheduling:
  - Shaped Round Robin (SRR) traffic shaping to mix packets from all queues to minimize traffic burst
  - Class-based traffic shaping to specify a maximum permitted average rate for a traffic class
  - Port shaping to specify the maximum permitted average rate for a port

  - Class-Based Weighted Fair Queuing (CBWFQ) to control bandwidth to a traffic class
  - WTD to adjust queue size for a specified traffic class
  - Low-latency priority queuing to allow preferential treatment to certain traffic
- Per-port, per-VLAN QoS to control traffic carried on a user-specified VLAN for a given interface. You can use hierarchical policy maps for per-VLAN classification and apply the per-port, per-VLAN hierarchical policy maps to trunk ports.
- Option to disable CPU protection to increase the available QoS policers from 45 to 64 per port (63 on every fourth port)

## Layer 2 VPN Services

The CGR 2010 ESM provides the following Layer 2 VPN services:

- 802.1Q tunneling enables service providers to offer multiple point Layer 2 VPN services to customers
- Layer 2 Protocol Tunneling (L2PT) to enable customers to control protocols such as BPDU, CDP, VTP, LACP, and UDLD protocols to be tunneled across service-provider networks

## Layer 3 Services

The CGR 2010 ESM provides the following Layer 3 services:

**Note** Layer 3 features are only available when the switch module is running the IP services image.

- HSRP Version 1 (HSRPv1) and HSRP Version 2 (HSRPv2) for Layer 3 router redundancy
- IP routing protocols for load balancing and for constructing scalable, routed backbones:
  - RIP Versions 1 and 2
  - OSPF
  - EIGRP
  - BGP Version 4
  - IS-IS dynamic routing
  - BFD protocol Bidirectional Forwarding Detection (BFD) Protocol to detect forwarding-path failures for OSPF, IS-IS, BGP, EIGRP, or HSRP routing protocols
- IP routing between VLANs (inter-VLAN routing) for full Layer 3 routing between two or more VLANs, allowing each VLAN to maintain its own autonomous data-link domain
- Policy-Based Routing (PBR) for configuring defined policies for traffic flows
- Static IP routing for manually building a routing table of network path information
- Equal-cost routing for load balancing and redundancy
- Internet Control Message Protocol (ICMP) and ICMP Router Discovery Protocol (IRDP) for using router advertisement and solicitation messages to discover the addresses of routers on directly attached subnets

- Protocol-Independent Multicast (PIM) for multicast routing within the network, allowing for devices in the network to receive the multicast feed requested, and for switches not participating in the multicast to be pruned. Includes support for PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM sparse-dense mode.
- Support for the SSM PIM protocol to optimize multicast applications, such as video
- Multicast Source Discovery Protocol (MSDP) for connecting multiple PIM-SM domains
- DHCP relay for forwarding UDP broadcasts, including IP address requests, from DHCP clients
- DHCP for IPv6 relay, client, server address assignment and prefix delegation
- IPv6 unicast routing capability for forwarding IPv6 traffic through configured interfaces using static routing, RIP, or OSPF
- IPv6 Default Router Preference (DRP) for improving the ability of a host to select an appropriate router
- Support for EIGRP IPv6, which utilizes IPv6 transport, communicates with IPv6 peers, and advertises IPv6 routes

## Layer 3 VPN Services

The CGR 2010 ESM provides the following Layer 3 VPN services:

**Note** These features are available only when the switch module is running the IP services image.

- Multiple VPN Routing and Forwarding (multi-VRF) instances in customer edge devices (multi-VRF CE) to allow service providers to support multiple VPNs and overlap IP addresses between VPNs
- Multicast Virtual Routing and Forwarding (VRF) Lite for configuring multiple private routing domains for network virtualization and virtual private multicast networks
- VRF and EIGRP compatibility

## Monitoring Features

The CGR 2010 ESM provides the following monitoring features:

- Switch Module LEDs that provide port and switch module-level status
- MAC address notification traps and RADIUS accounting for tracking users on a network by storing the MAC addresses that the switch module has learned or removed
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) for traffic monitoring on any port or VLAN
- SPAN and RSPAN support of Intrusion Detection Systems (IDS) to monitor, repel, and report network security violations
- Four groups (history, statistics, alarms, and events) of embedded RMON agents for network monitoring and traffic analysis
- Syslog facility for logging system messages about authentication or authorization errors, resource issues, and time-out events
- Layer 2 trace route to identify the physical path that a packet takes from a source device to a destination device

- Time Domain Reflector (TDR) to diagnose and resolve cabling problems on copper Ethernet 10/100 ports
- SFP module diagnostic management interface to monitor physical or operational status of an SFP module
- Online diagnostics to test the hardware functionality switch module while the switch module is connected to a live network
- On-board failure logging (OBFL) to collect information about the switch module and the power supplies connected to it
- Enhanced object tracking for HSRP clients (requires IP services image)
- IP Service Level Agreements (IP SLAs) support to measure network performance by using active traffic monitoring
- IP SLAs EOT to use the output from IP SLAs tracking operations triggered by an action such as latency, jitter, or packet loss for a standby router failover takeover
- EOT and IP SLAs EOT static route support to identify when a preconfigured static route or a DHCP route goes down
- IP SLAs for metro Ethernet using 802.1ag Ethernet Operation, Administration, and Maintenance (OAM) capability to validate connectivity, jitter, and latency in a metro Ethernet network
- Embedded event manager (EEM) for device and system management to monitor key system events and then act on them though a policy
- Support for EEM 3.2, which introduces event detectors for Neighbor Discovery, Identity, and MAC-Address-Table
- Support for the TWAMP standard for measuring round-trip network performance between any two devices that support the protocol

# Default Settings after Initial Switch Module Configuration

The CGR 2010 ESM is designed for plug-and-play operation - you only need to assign basic IP information to the switch module and connect it to the other devices in your network. If you have specific network needs, you can change the interface-specific and system-wide settings.

**Note** For information about assigning an IP address by using the browser-based Express Setup program, see the *Cisco Connected Grid 10-Port Ethernet Switch Module Interface Card Getting Started Guide*. For information about assigning an IP address by using the CLI-based setup program, see Appendix A, “Initial Configuration with the CLI Setup Program.”

If the CGR 2010 ESM is not configured, it operates with the default settings as shown in Table 1-3.

***Table 1-3 Default Settings After Initial Switch Module Configuration***

| Feature | Default Setting | More information in... |
|---|---|---|
| Switch Module IP address, subnet mask, and default gateway | 0.0.0.0 | Chapter 4, “Assign the Switch Module IP Address and Default Gateway” |
| Domain name | None | |

*Table 1-3 Default Settings After Initial Switch Module Configuration (continued)*

| Feature | Default Setting | More information in... |
|---|---|---|
| Passwords | None defined | Chapter 6, "Administer the Switch Module" |
| TACACS+ | Disabled | |
| RADIUS | Disabled | |
| System name and prompt | Switch | |
| NTP | Enabled | |
| DNS | Enabled | |
| MODBUS TCP | Disabled | Chapter 16, "MODBUS TCP Configuration" |
| 802.1x | Disabled | See "Configuring IEEE 802.1x Port-Based Authentication" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/sw8021x.html) |
| **DHCP** | | |
| DHCP client | Enabled | Chapter 4, "Assign the Switch Module IP Address and Default Gateway" |
| DHCP server | Enabled if the device acting as a DHCP server is configured and is enabled | |
| DHCP relay agent | Enabled (if the device is acting as a DHCP relay agent and is configured and enabled) | See "Configuring DHCP Features and IP Source Guard" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swdhcp82.html) |
| **Port Parameters** | | |
| Port type | Gigabit Ethernet: NNI, Fast Ethernet ports: NNI | Chapter 8, "Interface Configuration" |
| Operating mode | Layer 2 (switchport) | |
| Port enable state | Enabled for NNIs; disabled for UNIs and ENIs | |
| Interface speed and duplex mode | Autonegotiate | |
| Auto-MDIX | Enabled | |
| Flow control | Off | |
| Command Macros | None configured | Chapter 10, "Smartports Macros Configuration" |
| **VLANs** | | |

*Table 1-3 Default Settings After Initial Switch Module Configuration (continued)*

| Feature | Default Setting | More information in... |
|---|---|---|
| Default VLAN | VLAN 1 | Chapter 11, "VLAN Configuration" |
| VLAN interface mode | Access | |
| VLAN type | UNI isolated | |
| Private VLANs | None configured | Chapter 12, "Private VLAN Configuration" |
| Dynamic ARP inspection | Disabled on all VLANs | See "Configuring Dynamic ARP Inspection" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swdynarp.html) |
| **Tunneling** | | |
| 802.1Q tunneling | Disabled | Chapter 13, "IEEE 802.1Q and Layer 2 Protocol Tunneling Configuration" |
| Layer 2 protocol tunneling | Disabled | |
| **Spanning Tree Protocol** | | |
| STP | Rapid PVST+ enabled on NNIs in VLAN 1 | See "Configuring STP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swstp.html) |
| MSTP | Disabled (not supported on UNIs, can be configured on ENIs) | See "Configuring MSTP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swmstp.html) |
| Optional spanning-tree features | Disabled (not supported on UNIs, but it can be configured on ENIs) | See "Configuring Optional Spanning-Tree Features" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swstpopt.html) |
| Resilient Ethernet Protocol | Not configured | See "Configuring Resilient Ethernet Protocol" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swrep.html) |
| Flex Links | Not configured | See "Configuring Flex Links and the MAC Address-Table Move Update Feature" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swflink.html) |
| **DHCP Snooping** | Disabled | |
| IP source guard | Disabled | See "Configuring DHCP Features and IP Source Guard" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swdhcp82.html) |

*Table 1-3 Default Settings After Initial Switch Module Configuration (continued)*

| Feature | Default Setting | More information in... |
|---|---|---|
| **IGMP Snooping** | | |
| IGMP snooping | Enabled | See "Configuring IGMP Snooping and MVR" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swigmp.html) |
| IGMP filters | None applied | |
| IGMP querier | Disabled | |
| MVR | Disabled | |
| IGMP throttling | Deny | |
| **Port-based Traffic Control** | | |
| Broadcast, multicast, and unicast storm control | Disabled | See "Configuring Port-Based Traffic Control" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swtrafc.html) |
| Protected ports | None defined | |
| Unicast and multicast traffic flooding | Not blocked | |
| Secure ports | None configured | |
| CDP | Enabled on NNIs, disabled on ENIs, not supported on UNIs | See "Configuring CDP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swcdp.html) |
| LLDP | Disabled (not supported on UNIs) | See "Configuring LLDP and LLDP-MED" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swlldp.html) |
| UDLD | Disabled | See "Configuring UDLD" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swudld.html) |
| SPAN and RSPAN | Disabled | See "Configuring SPAN and RSPAN" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swspan.html) |
| RMON | Disabled | See "Configuring RMON" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swrmon.html) |
| Syslog messages | Enabled; displayed on the console. | See "Configuring System Message Logging" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swlog.html) |
| SNMP | Enabled; Version 1 | See "Configuring SNMP" (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swsnmp.html) |

*Table 1-3 Default Settings After Initial Switch Module Configuration (continued)*

| Feature | Default Setting | More information in... |
|---|---|---|
| ACLs | None configured | See “Configuring Network Security with ACLs” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swacl.html) |
| QoS | Not configured | Chapter 14, “Quality of Service Configuration” |
| EtherChannels | PortChannel 48 | Chapter 9, “EtherChannel Configuration Between the Switch Module and the Host Router” |
| **IP Unicast Routing** | | |
| IP routing and routing protocols | Disabled | See “Configuring IP Unicast Routing” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swiprout.html) |
| Multi-VRF-CE | Disabled | |
| HSRP groups (requires IP services image) | None configured | See “Configuring HSRP” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swhsrp.html) |
| Cisco IOS IP SLAs | Not configured | See “Configuring Cisco IOS IP SLAs Operations” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swipsla.html) |
| Enhanced object tracking | No tracked objects or list configured | See “Configuring Enhanced Object Tracking” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/sweot.html) |
| IP multicast routing (requires IP services image) | Disabled on all interfaces | See “Configuring IP Multicast Routing” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swmcast.html) |
| MSDP (requires IP services image) | Disabled | See “Configuring MSDP” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swmsdp.html) |
| **Ethernet OAM** | | |
| CFM | Disabled globally, enabled per interface | See “Configuring Ethernet OAM, CFM, and E-LMI” (http://www.cisco.com/en/US/docs/switches/connectedgrid/cgs2520/software/release/12_2_53_ex/configuration/guide/swoam.html) |
| E-LMI | Disabled globally | |
| Ethernet OAM protocol (802.3ah) | Disabled on all interfaces | |

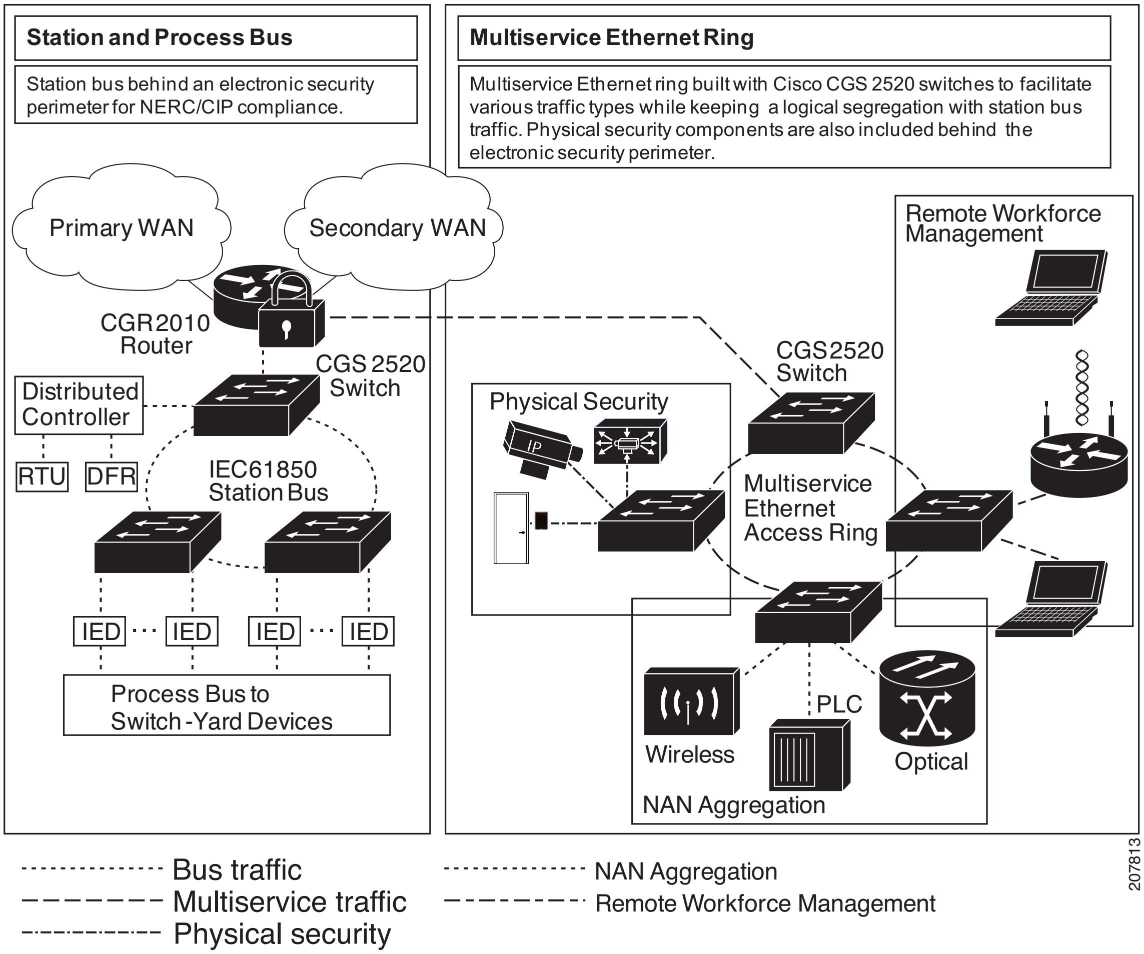
# Utility Substation Application

Cisco CGR 2010 routers and the CGR 2010 ESM are designed for use in Transmission and Distribution (T&D) power substations. Figure 1-4 shows a partially redundant, multiservice configuration for deployment in a utility substation environment.

A substation router, such as a Cisco CGR 2010 router, defines the Electronic Security Perimeter (ESP) for the substation. The station bus network and multiservice network are located behind the substation router. The station bus network employs a ring topology for a resilient, redundant network and connects to different substation devices such as IEDs.

The multiservice network is virtually segmented from critical SCADA control traffic and supports services such as remote workforce management, physical security, and Field Area Network (FAN) aggregation. Advanced QoS capabilities support mission-critical substation traffic such as SCADA, and generic GOOSE messages, and ensures that substation network traffic is prioritized ahead of the multiservice network traffic.

***Figure 1-4 CGR 2010 ESM in a Utility Substation Application***


Station and Process Bus
Station bus behind an electronic security perimeter for NERC/CIP compliance.
Multiservice Ethernet Ring
Multiservice Ethernet ring built with Cisco CGS 2520 switches to facilitate various traffic types while keeping a logical segregation with station bus traffic. Physical security components are also included behind the electronic security perimeter.
Primary WAN
Secondary WAN
CGR2010 Router
CGS 2520 Switch
Distributed Controller
RTU
DFR
IEC61850 Station Bus
IED
IED
IED
IED
Process Bus to Switch-Yard Devices
Remote Workforce Management
CGS2520 Switch
Physical Security
IP
Multiservice Ethernet Access Ring
PLC
Wireless
Optical
NAN Aggregation
207813
Bus traffic
Multiservice traffic
Physical security
NAN Aggregation
Remote Workforce Management

# Where to Go Next

Before configuring the switch module module, review these chapters for startup information:

- Chapter 2, "Command Line Interface"
- Chapter 4, "Assign the Switch Module IP Address and Default Gateway"
- Chapter 5, "Cisco IOS Configuration Engine"

- Chapter 9, “EtherChannel Configuration Between the Switch Module and the Host Router”